c:\nucs\c3.60
9 August 1989

Comments on my August 1960 paper, Strategic Objectives and Command Control Problems, Rand D-7838

--Note: This was written during my and RAND's "missile gap" concern; though it was about the time that Andy Marshall had begun to hint to me and a few others (including an advisory group for Kennedy's campaign) that "there might be no missile gap after all." (He could give us no reasons for this prediction, which ran totally counter to the assumptions of RAND and USAF studies).

--This was written after my work for CINCPAC and my reading of the war plans--including, I presume, the JSCP, though I'm not certain of that at this moment. Yet the definition of "general war" on p. 14--"the all-out struggle to the finish between the United States and the USSR"--reflects the general understanding of that term, not the highly secret definition in the JSCP: "armed conflict between the US and the USSR," which deliberately excluded the notion of limited war with the Soviet Union or any strategy in such a conflict other than the immediate execution of what came to be called the SIOP. (I may simply have been keeping the secret--especially in this unclassified D--of this latter definition, which it was my goal to bring to the attention of the Secretary of Defense and the President).

--p. 19. The JSCP and SIOP-62 that ruled at the outset of the Kennedy Administration were indeed designed to operate "on the principle of the mousetrap; given certain preselected triggering signals, a predetermined, inexorable response would follow fast and automatically (without "feedback control")."

This mousetrap was designed and expected to kill promptly some 600 million people.

Perhaps more than I appreciated at the time, this design may have reflected a tacit understanding by the JCS and SAC Commanders of the vulnerability of command centers and communications, and thus the near-impossibility of either centralized or decentralized post-attack control.

Another factor that I didn't fully recognize at the time was the degree to which General LeMay and his disciples felt post-attack control was unnecessary, in view of their belief that a single target system was optimal under all circumstances, both for deterrence, retaliation and war-fighting.

That is, it was not till I saw the continuous lineage of the 1959-60 plans from the World War II attacks on Japan through the nuclear plans of the late `40's (before there was any threat of Soviet nuclear attack) and the early `50's, when the threat of Soviet attack was still minimal, that I fully realized that, to

LeMay, Soviet cities were suitable and critical first-strike targets.

Moreover, they were suitable "prompt" targets for the first wave of attack, along with Soviet nuclear bases and other military targets. The desirability of attacking them immediately was reinforced by the above consideration, that any Soviet retaliation at all was likely to eliminate US command and control. Third, any delay in attacking them could tempt a US President, if he were still alive, to decide against attacking them at all: eliminating what LeMay saw as a crucial part of a war-winning strategy. Fourth, Moscow in particular was the center of the Soviet command and control system, which LeMay sought to destroy at the outset.

Preserving Soviet command and control in hopes of bringing about an end of the war--without full expenditure of Soviet forces--held no advantages to the JCS or SAC, in their knowledge--not shared with RAND or me (or the President)--that Soviet forces were so small even before US attack, and so vulnerable, that this "coercive option" which I prescribed in my draft guidelines in 1961 was not a compelling strategy for dealing with any Soviet residual forces. (My coercive strategy presumed that fairly large, relatively invulnerable Soviet forces were to be expected to survive the first nuclear exchange; this was the implication of official CIA/USAF intelligence estimates).

Thus the only military objective in general war (in the usual, non-JSCP sense) was to destroy as promptly as possible a fixed target system, which played the role, in effect, of the mouse. LeMay was the exterminator of the mouse,

D-7836

August 12, 1960

Assigned to _____

LIMITED

FOR RAND USE ONLY

NOT TO BE QUOTED OR CITED IN EXTERNAL RAND PUBLICATIONS OR CORRESPONDENCE

PREFACE

What are "the problems" of the human nervous system? In a structure so delicate and complex, its functionings critical to every aspect of behavior, the list of potential "problems" is endless. It is a similar challenge to specify the problems of military command and control systems, the nervous system of the military organization. Even when the principles of selection are made explicit, any such list will inevitably bear a personal imprint, reflecting individual judgment, experience and interest.

The particular problems isolated for discussion in this paper are those which seem most critical to the feasibility or degree of attainment of certain national strategic objectives: deterrence, stability, improved war outcome. In fact, it is the interaction between strategic objectives and the characteristics of command control systems -- in particular, the "post-attack" capabilities -- which is the principal subject of this paper. More expository material on general problems has been included than if the paper were addressed solely to those experienced in the field; I have tried, in part, to produce the sort of paper that would have been helpful to me, on matters of relevance, importance and strategic implications, at the time when my own serious interest in the subject first began.

A particular command and control system may be analyzed in terms of various system characteristics; N. Dalkey has suggested the list: Cost, Vulnerability, Flexibility, Sensitivity, Reliability, Reaction Time. Again, its contribution to alternative possible sets of military objectives can be evaluated (that will be the focus of this paper). Or its feasibility and effectiveness can be estimated with respect to different hypothetical environments, threats, challenges. There may be room for reasoned argument

over every one of these judgments; and reasonable men will certainly disagree over the relative importance of the various tests.

It is not the purpose of this paper to try to settle either sort of controversy, but to expose the outlines of the debate, the issues and conflicting criteria which give rise to disagreement. It is meant to provide incentive, and to some extent guidance, to research. Where there is a tone of advocacy in the following pages, it attaches not to "solutions" but to the importance of problems, objectives, research needs. And even these judgments are individual; the editorial "we" throughout does not necessarily indicate any consensus of opinion within discussion groups to which this paper has been an input.

However, as this paper has gone through several versions, it has benefited by an unusual amount of helpful criticism. To say that the list of additional critics of earlier drafts is "too long to mention" is almost true, but that would not do justice to my appreciation for their efforts. The members of the Committee on Command and Control Problems under John Williams and the subsequent Advisory Group on Command and Control were particularly helpful; these included N. Dalkey, F. Eldridge, W. Ware, H. Goldhamer, C. Zwick, R. Specht, J. Carne, R. Van Horn, and J. Digby. R. Eldridge, R. Radner, M. Geisler, W. Steger, N. Jordan, R. Brock, J. Bower, H. Rowen, A. Carlin, and A. Marshall all did me the favor of commenting extensively. The remarks on counterforce are particularly influenced by discussion with A. Marshall, and those on threat strategies by conversation with and the writings of Marshall, H. Goldhamer, T. C. Schelling and H. Kahn. On problems of command and control in general, I am particularly indebted to F. Eldridge, Carne and Dalkey;

talks with T. Reade, H. Bennington and A. Barber of the Winter Study Group were also helpful. Overall, the paper reflects in large part research undertaken as a member of the ONR Study Group on PACOM Information and Control under J. Wilkes of ONR.

After this acknowledgment, it is necessary to reiterate that although the present version of this paper has been heavily, and usefully, influenced by criticism from all these people, the influence has not always been in the direction which they would have wished, so that they are in no way responsible for its contents; undoubtedly, many disagreements remain, both on points of emphasis and substance.

This paper is being considered for possible publication as an RM. I would therefore appreciate receiving criticism of all sort, including omissions, suggestions for cutting, and useful references.

CONTENTS

STRATEGIC OBJECTIVES AND COMMAND CONTROL PROBLEMS

Daniel Ellsberg

INTRODUCTION

"Command and control" is a central process within the military organization, the process of planning and directing military operations. It entails gathering information on the external threat, the status and capabilities of friendly forces; communicating and processing this information and analyzing its relevance to decision-making; choosing a course of action; translating this into specific orders and transmitting them; and controlling their execution. Or, as J. Carne has summarized the process, it consists of perceiving what is happening, deciding what to do, and carrying out these decisions.

The overall system that serves the command and control process encompasses people, plans, operational procedures and communications and data-processing hardware; its anatomy includes a complex pattern of authority and a network of information flows. It can accurately be described as the nervous system of the military organization.

This is to use the term "command and control system" in a much broader sense than the one which is common to much current discussion: a large, highly automated system of electronic data-processing equipment and associated communication network designed to provide commanders promptly with information needed for decision making, and to assist them in implementing their decisions. In this latter, narrow sense, proposed "Command Control Systems" range from those, like BMEWS, satellite reconnaissance and various intelligence systems, which primarily supply

data on the external environment and enemy threat, to those which provide information on status of forces and allow for some control of weapons systems. In the context of these proposals, "command and control problems" are problems arising from these Command and Control Systems: in particular, from their relations with each other. These are problems of the efficient organization of large systems of computers and automated communications equipment: data-rate, efficient data-sharing, compatibility of computer languages, coordination, avoidance of unnecessary duplication, transition problems and the orderly evolution of the system.

In the broad terms of our discussion here, "command and control problems" are any problems associated with the actual or desired characteristics of the military nervous system. These characteristics are so critical in determining military capabilities that a given command and control system can have an important influence on the feasibility, hence the selection, of national military objectives and strategies. On the other hand, a given set of national military objectives or strategies will imply definite requirements for command control capabilities to implement them. We will focus, in this paper, chiefly upon this interrelationship between national military strategic objectives and the required or actual properties of the command and control system.

The frequent neglect of this interaction may stem from a belief that it "should not" hold: that command and control system design must aim at total flexibility, compatibility with any objectives or strategies whatever, and total lack of limitational constraint upon the behavior of the military organization. And indeed, it is tempting to imagine a

command and control system which would free national strategy from any such constraint: a system so flexible, reliable and quick-reacting that the only restraints on action in pursuit of freely chosen objectives would be set by the physical characteristics of the forces and the environment.

Yet this seems an unrealistic goal. Worse, it discourages careful analysis of the actual relationships between given goals, tactics and command systems. Ironically, it can thereby result in proposed systems designs which would place -- unwittingly -- the most extreme constraints upon organizational goals and behavior.

It seems likely that the precise characteristics of the military nervous system -- its vulnerability, sensitivity, discrimination, reliability, speed, capacity -- will always set some limitations on the likely or feasible behavior of the military organization, on the flexibility and speed of military response. Messages will always take time in transmission; perfect reliability for all messages will not be achieved; there will always be some limit on data-processing capacity and the dissemination of information; neither commanders, computers nor communications will be rendered strictly immortal; thermonuclear explosions will always promise some deleterious effect on the functioning of the military nervous system. What is important is to know clearly the precise constraints implied by a given system; to evaluate their significance to national military objectives; and to attempt to modify those constraints that seem least tolerable.

In this discussion, we shall concentrate upon those problem-areas where the interdependence of strategic objectives and command capabilities

shows up most clearly; this leads to an emphasis upon wartime problems. The discussion will be somewhat abstract. In speaking of the preservation under attack of some form of the command and control process, we shall be referring to the preservation of certain functions. This will surely entail the preservation of some sort of communications and computational hardware, of sensors, of commanders as people. But little will be said here as to just what specific items and organizational forms might best serve these functions in a post-attack environment. There are many important problems which receive little or no attention in this paper, for reasons which do not reflect upon their relative significance. Some examples are: control during limited war; organizational problems (e.g., the role of service headquarters in the command system, the distribution of certain functions among various levels of command); problems of hardware and implementation (e.g., what means are best for assuring survival of certain functions, how "hard" should particular components be made).

In the first section, we will discuss some of the critical challenges to the functioning of the command and control system, particularly in wartime. This may serve as introduction to the subject for those who are unfamiliar with command and control problems. For those who have been working in this field, some of the propositions will be monotonously familiar; they may prefer to skim this section. Yet it may not be quite truistic to assert that these propositions define important "problems." Not every unpleasant fact constitutes a "problem"; that will depend upon its implications for actions and goals, the importance and the feasibility of modifying it. It is a fact that humans do not live to two hundred,

but that would not be listed among the "problems" facing medical science; it is not considered important to live that long, and it looks impossible. Similarly, there are experts who are quite familiar with the facts that commanders and communications are highly vulnerable under nuclear attack, but who might fail to regard these as highly important "problems." Given sufficient pessimism or sufficiently restricted strategic objectives, this view is quite justified; these limitations become problems only when strategic objectives are extended, e.g., beyond pure deterrence based upon the threat of punitive retaliation. A command and control structure quite adequate to this latter objective might be totally inadequate for fighting a war if deterrence failed, for achieving such objectives as limiting damage to the United States or achieving a satisfactory end to the war. In the second, longer section we will explore such relationships between strategic objectives and command and control structures.

I

SOME "COMMAND AND CONTROL PROBLEMS"

Commanders have always had problems.

Uncertainty has always beset their decisions; every commander since Alexander, and before, has acted within "the fog of war." Their information comes to them incomplete, ambiguous, of varying and uncertain reliability; and always it comes late. "But what is happening at the battlefronts now?" There has never been a way to tell them. Messages, disappointingly like planes and infantry, take time to travel. The time required for handling and interpreting information, for making decisions, generating plans and transmitting orders has always been significantly long compared to the time "available": the interval within which the information is relevant, the plans and orders appropriate.

There has never been (nor is there now) just one "command and control problem." There has never been staff during peace, nor time during war, for truly varied contingency planning. (Both the French and the Germans in World War I had a library of one basic war plan.) In fixing the locus of effective operational command, there has always been the conflict between the claims of the local commander, with his concrete, detailed and immediate knowledge of local conditions and enemy threat, and those of the over-all commander with his broader access to information (more varied, but less detailed and possibly stale) and more intimate knowledge of national objectives.

The tasks of evaluating complex alternatives and choosing, of predicting the effectiveness of untried weapons and tactics against an uncertain threat, have never been easy. As armies have grown larger -- and they have always been large in relation to the tools of communication and

decision available for managing them -- the problems of controlling their execution of chosen strategies have multiplied. These are problems familiar to any large organization, of finding out what subordinate units are actually doing and how they are succeeding, of re-directing and coordinating their efforts: but compounded, in a military organization in wartime, by the time-pressure of combat, by an unfamiliar and rapidly changing environment, and by the efforts of an enemy to disrupt control.

In past wars high commanders have not frequently been killed, but they have been abruptly fired and replaced with others unfamiliar with the staffs and with the course of conflict, they have lost communications, they have had to wait out periods when their forces and the battle were "out of control." And they have been asked to make choices, under such circumstances, on a scale to which no man, neither statesman nor general, has been equipped to do full justice. Always it has been their task to make decisions -- fast, and lacking certain knowledge -- upon the lives of men, the death of cities, the history of nations.

These problems of command are age-old. What is so special or new about the current ones?

The differences, perhaps, are only in degree; but some of these are startling. From another point of view, some of the problems seem "new" not in relation to an old tradition but to the trend of recent past experience, which suggested that the aids to effective high-level command (improved and speedier reconnaissance, reliable fast communications) might outrun the obstacles. That trend was halted -- some think, irrevocably reversed -- with the emergence of thermonuclear warheads and very fast, long-range delivery means. It is the ominous, poorly-discerned outlines

of thermonuclear war that dominate contemporary consideration of problems of command and control.

Some of these problems have long been familiar at tactical levels of command; what seems new is that they appear now at the highest national levels. To paraphrase a vivid analogy by John Williams: in future war the command process at the national level might experience challenges heretofore more familiar to a rifle platoon in an assault. Within a timespan of minutes, commitments may become irrevocable, unavoidable tragedies take place, major opportunities may appear and vanish, errors of judgment have their effect. If the leader survives, he may be out of communication with his scattered units for important intervals. And the leader himself may die in the first minutes of combat.

In the past, Williams points out, the outcome of war has depended upon many thousands of such brief actions, and it could be favorable despite thousands of individual failures. In future, the fate of our nation, perhaps that of Western society, could depend on a small number of decisions -- or the lack of them -- made just so rapidly under such chaotic conditions.

So long as these problems of communications lags and outages, survival of commanders and strains on decision-making were most critical at tactical levels of command, they tended to <u>stay</u> problems; there was a tendency to "live" with them and adapt to them, rather than to devote major research and procurement effort to surmount them. It is when these constraints appear, in equally dramatic form, at national levels of decision that the problems come to seem new: because they seem no longer tolerable.

Whether or not, then, the problems are really new, it is a fact that in the past decade they have earned, and are receiving, heightened attention. And the basis for this is the prospective character of thermonuclear war.

Some Wartime Problems

(1) Vulnerability of command. For the first time in warfare, the highest national command posts and political decision centers are subject to direct, annihilating attack in the first moments of war. Indeed, the first warning that general war had started could take the form of "bomb alarm" signals from Washington, Omaha, Colorado Springs, and the headquarters of unified commands. This possibility jeopardizes the role of major decision-makers not only in the continued direction of hostilities but even in determining the initial response.

(2) Vulnerability of communications. Communications have always been frustratingly unreliable, especially at tactical levels. But nuclear weapons can effect widespread disruption of major communications systems in an unprecedented way. There are communication means that might survive such attacks, and more may be invented, but so may new weapons effects and enemy tactics appear to counter them.

The "sense of immortality" surrounding elaborate communications networks, with their multiplicity of channels, has been lost. A planner can no more be confident that "somehow," by some means or other over some circuitous route, a vital message will always get through: at least, without major and unpredictable delay. And given the tempo of nuclear

war, even the delays enforced by widespread damage to communications and consequent rerouting could be fatal.

(3) The tempo of operations. Current delivery means make possible a swift attack with thermonuclear warheads, giving little or no warning. Most military forces, including strategic weapons, are highly vulnerable so such attack. Hence, under nuclear attack, the status and capabilities of the forces on both sides can change with dramatic swiftness. An army, a fleet of bombers and supporting bases, a missile force, available for action one moment might, ten minutes or an hour later, have ceased to exist.

In other words, the tempo of major operations may speed up enormously. The period during which information on status, capabilities and enemy threat remains a timely, valid basis for decision may be drastically reduced; the relevance of given information may decay very rapidly.

To the extent that the survival of the offensive force depends upon fast response to warning, this problem of tempo appears most sharply in the initial moments of general war. To achieve the warning and response, a large amount of data must be processed and momentous decisions made with unprecedented speed. If the warning system fails and the enemy achieves surprise, most of the pre-attack data on status and capabilities of friendly forces may be outdated within minutes of the outset. If a choice at this point is to reflect remaining capabilities (which is controversial), again there is call for unprecedented speeds, though now for handling possibly smaller amounts of information.

It was this problem of the initial response in general war -- defined

thus, in the context of an offensive force highly vulnerable to surprise attack -- that gave recent discussions of command and control problems much of their urgency and that focused attention upon speed in communication and decision-making. This led naturally to interest in the contribution of computers and automated systems. But meanwhile, an era may be approaching in which an increasingly large fraction of the offensive force does not depend for its survival upon fast response to warning; and other motives for fast action may be lessening. Thus, although the problem of tempo is probably the best recognized and most discussed wartime problem of command and control, its importance may be diminishing relative to other problems.

(4) The unfamiliar and potentially cataclysmic nature of nuclear war. These strongly reinforce the traditional desire for centralized, high-level decision-making and control during hostilities, and for the flexibility to adapt to unexpected developments.

In any war, if it were technologically and organizationally feasible, the highest commander who was authorized to control operations would usually desire to do so. He will be responsible for decisions made in his command in any case; and to the extent that they may be momentous, he will wish his own judgment of uncertainties and interpretation of national objectives to be controlling. Moreover, he will typically possess information from a greater number of sources than any of his subordinate commanders.

These motives become far more compelling when decisions involve nuclear weapons. The costs of an accident or unauthorized use in peacetime or of a misdirected strike in wartime can be so great, a single

large nuclear explosion can have such momentous consequences, as practically to demand control from a center with the broadest access to political and military information and the clearest view of over-all national objectives. This requirement for centralized decision-making and "positive control" has been clearly recognized for peacetime (to avoid costs of destruction, loss of alliances, danger of war based on accident, unauthorized action or "false alarm"), for limited wars (to avoid undesired expansion), and for the initial response in general war (to minimize false alarms, to ensure appropriate strategy, to avoid retaliating against the wrong enemy in an era when many nations possess nuclear weapons). The case for some continued centralized control even during "central war" has been relatively neglected. We will consider the arguments, pro and con, affecting this in later sections; they have to do, for example, with the employment of threat-strategies, the ability to deal with unexpected developments, the problems of terminating the war, and the need for responsible political/military direction.

(5) The effective level of operational control. Although the conditions of thermonuclear war create incentives to flexible, informed, centralized control, at the same time they raise formidable obstacles to it, by magnifying the effects of delays in decision and by making commanders and communications vulnerable. In other words, the same weapons developments which have increased the desire of high commanders to concentrate control of operations in their own hands may drastically reduce the effectiveness or feasibility of their control.

It must take time for information to be collected and communicated to a higher level of command; it takes time for that command to process and correlate the information and interpret its implications for opera-

tions; more time for a decision to be reached and translated into specific orders; still more time for these orders to be transmitted to subordinate units; and a final wait before these units can respond. These inevitable delays -- communication lags, information-processing lags, decision-making lags, transmission and response lags -- determine the time required for decision-making and appropriate adaptation. The "tempo of operations," as we have been using this term, determines the time available. Given the lags relative to a certain level of command, then the faster the tempo of operations, the more difficult it becomes for that level of command to control operations in effective response to changing information. A speedup in tempo -- such as might correspond to the introduction of nuclear weapons -- tends to work against effective control by higher headquarters.

There are several ways of responding to this challenge. One is to forego effective control by high headquarters, delegating most or all decision-making to lower-level commands, thereby shortening communication, transmission and possibly information-processing lags, permitting more timely response. In some circumstances, it can be more effective for a local commander to act promptly upon his "good" knowledge of local conditions than to take time for a higher commander to bring to bear his broader but more superficial knowledge of general conditions. The advantages in over-all efficiency of this "decentralized" control of moment-to-moment operations may compensate to the high commander for the fact that some operational decisions will not only be divorced from his own judgment of conditions and objectives but may ignore some relevant information from other sectors.

Considerations of the vulnerability of commanders and communications encourage a more radical approach: minimizing any reliance whatever upon real "decision-making" at any level and upon the communication of information or directives during hostilities, since such processes may be fatally disrupted by the enemy. Vulnerability considerations favor increased reliance upon pre-hostilities planning, automatic dissemination of necessary information, and decentralized execution of appropriate plans. Proponents of this approach argue that the alternative to such a system, with all its limitations, may be one which not merely tends to respond too late: it may not respond at all.

Whatever the merits of decentralization and "automation," with respect to speed and vulnerability, it is a fact that their limitations in terms of responsible, informed control and adaptability can be very serious.

Thus the advent of nuclear weapons pulls in two directions on the "optimal" locus of operational control. These problems are not limited to "general war," the all-out struggle to the finish between the United States and the USSR, or even to what has been called "central war," involving attacks on the opposing homelands. Any war involving nuclear weapons creates the incentives for flexible, responsible, centralized direction. At the same time it can bring, at least in certain stages, abrupt changes in status and capabilities that require rapid information-gathering and decision-making; and it introduces the vulnerability of commanders (e.g., subordinate commanders) and communications.

Two other sorts of developments may help to mitigate this conflict. Advances in information-processing techniques, communications, computers,

displays, planning techniques and protective measures may reduce many of the crucial lags and command system vulnerabilities, restoring the effectiveness of high-level control. And progress in protecting weapons systems -- on both sides -- may considerably lessen the expected tempo of operations.

Indeed, given the advances alone in surveillance, communications and data-processing -- without the new weapons -- the coming decade would offer promises rather than problems for commanders. In a war of "old-fashioned" tempo -- like World War II -- a high commander could exercise more detailed and efficient control of operations than ever before. But the increase in tempo, it will be argued, may have outrun these advances; and what is even more to the point, there have not been comparable advances yet in countering the vulnerability problems.

Technical developments which increase the amount of information which a given headquarters can receive, process, interpret and transmit in a given time interval permit the high-level control which will often be urgently desirable, but at the same time they increase the feasibility of effective decentralized control of certain functions. This permits a flexible approach to the problem of operational control, with some functions centrally controlled and others decentralized. Thus, some of the decision-making and information-processing load can be removed from the higher headquarters, and lags reduced, by transferring certain decisions to subordinate commands and by developing a library of contingency plans and interpretative criteria for decision-making, to the effect that remaining, critical functions can be handled more effectively by the higher command.

To the extent that one believes that all important decisions can be delegated or preplanned, then the vulnerability of commanders and communications, the pressures on wartime decision-making and the incentives for responsible direction cease to be "problems." And there are those who approach this belief. We have dwelt at length on what may seem familiar propositions to emphasize a contrary point of view, that these propositions do specify important "problems," highly deserving of research resources and effort. Later sections will spell out the serious limitations imposed on the behavior and goals of a military organization which lacks a capability for adaptive, responsible post-attack control.

Some Peacetime Problems

Partly because the wartime problems seem so intractable, partly for other reasons considered in the next section, interest in command and control has, in fact, centered upon peacetime, pre-hostilities problems. Although the focus of this paper is upon wartime problems, the peacetime problems deserve mention not only because they loom so large in current discussion but because they are interrelated with the wartime problems with which they compete for attention.

The pre-hostilities problems, too, are dominated by the portents of thermonuclear war. The vulnerability of current forces to nuclear surprise attack has conferred immense advantages upon the side that strikes first; it is generally assumed that the side striking second has few prospects of coming out well no matter how it conducts the war. This has led to great emphasis on peacetime upon the deterrence of surprise attack, based on the deterrent threat of immediate, all-out retaliation. Given the vulnerability of its strategic forces to attacks giving little or no

warning, the United States has tried to support its threat of assured retaliation with a capability for tactical warning and for fast response. Hence, the objective of deterrence has had as corollaries:

- The maintenance of a large peacetime force in being, distributed globally (principally bombers and tankers, but evolving into a mixed force of planes and missiles, based on and beneath the land and sea or "continuously" airborne);
- The maintenance of a large part of the force in a high constant state of readiness, and the requirement of detailed, up-to-the-minute knowledge of force status and capabilities, target and strike data;
- A need for a continual, massive influx of intelligence, surveillance, and early-warning data to be processed and evaluated with high speed;
- The importance of detailed, pre-hostilities planning for contingencies, to permit fast response and to allow for the wartime vulnerability of commanders and communications and constraints upon wartime decision-making capability.

Each one of these conditions has generated requirements for data-collection, and for data-processing, communication and planning facilities, on a scale unprecedented in peacetime. In some respects this trend toward voracious data-processing may slow down. The data requirements for the maintenance, control and coordination of missiles may be less than those for bombers and tankers. As an increasing portion of the force becomes less vulnerable to surprise attack, the emphasis upon tactical warning and immediate response may somewhat diminish.

On the other hand, each of the above conditions may persist, no matter how far the capabilities for wartime decision-making and control may be developed. Not only will deterrence, based on force posture and readiness, continue to be a preeminent goal, but wartime capabilities will be strongly dependent on peacetime preparations: on alerting

activities triggered by warning, on the provision and updating of information and on flexible, varied contingency plans. It is essential to exploit to the limit the large, undamaged capabilities of the pre-attack command system and communications in an effort to ease the decision-making burden of commanders operating in a post-attack environment.

Nor are the technological problems of wartime and peace entirely separate. Although it is the peacetime problems, in particular, that favor electronic data-processing systems for the cost-efficient transmission and processing of large volumes of data, some important wartime problems may likewise demand automated systems and sophisticated data-processing equipment. However, a wartime system must pass a test which a system designed primarily for a peacetime environment will almost surely fail: it must be able to survive attack.

If command facilities and communications were to be totally vulnerable, there would indeed be a split between the wartime and the peacetime "problems." In the pre-attack phase of operations, commanders would face a deluge of data; their problem might be to avoid being overwhelmed by it. At the moment of attack the stream of data, produced by vulnerable sensors, churned, directed and sped on its way by elaborate but unprotected electronic systems, could be shut off as abruptly as by the flicking of a switch. The post-attack phase would proceed, then, in a total drought of data: lacking sensors, systems, communications or commanders. These conditions would apply all up and down the hierarchy of command. There is no question here of "centralized" versus "decentralized" control of operations; such a system would offer no

post-attack control.

An attempt might be made to justify this system in terms of an over-all strategy which "solves" the wartime problems by by-passing them: by designing a wartime response which is quite independent of the survival or functioning of commanders and communication beyond the opening minutes of major nuclear war. Such a system would act on the principle of the mousetrap; given certain preselected triggering signals, a predetermined, inexorable response would follow fast and automatically (without "feedback control").

This strategy would emphasize those functions of commanders that can be performed prior to attacks upon command and communications: pre-hostilities planning, the maintenance of a deterrent posture, transmission, if deterrence fails, of an appropriate "Execute" message based upon a prior contingency plan. The approach is not without its wartime problems; some proposed systems, following this pattern, seem all too likely to fail under surprise attack even before the transmission of a "Go" order. But by relying upon the automated execution of a prior plan, this strategy does promise to minimize reliance upon commanders and communications during hostilities.

There are arguments to be made for this "solution." Perhaps the strongest is the difficulty of providing a feasible alternative. Yet it seems important to try to do so; the "mousetrap" strategy should not win by default.

A complex, highly-automated -- and highly vulnerable -- data processing system, of the sort described above, might or might not prove adequate to meet the new peacetime problems. But could it provide an adequate

solution to the wartime problems? Can all the major problems of wartime control be transformed effectively into pre-hostilities problems, by relying upon preplanning, automated alerting and automatic or decentralized execution? Arguments will be advanced later in this paper that this solution cannot be satisfactory.

Pre-attack problems are important; they include deployment, planning, posture maintenance and alerting, the conduct of operations in limited wars involving no large-scale destruction of command or communications and in the initial moments of major nuclear war prior to such destruction. And surely, what is possible in wartime will depend upon the capabilities of the peacetime system, and the use made of those capabilities. But it will be argued that no development of pre-hostilities capabilities can wholly compensate, in terms of important strategic objectives, for an essentially total paralysis of the military nervous system under enemy attack.

II

STRATEGIC OBJECTIVES AND COMMAND AND CONTROL SYSTEMS

It seems likely that in the 'Sixties, and probably in the 'Seventies, we will not be able to have everything we would like in the way of command capability. The task of system design will require rigorous analysis and some painful choices.

It is all the more important to be clear as to what we would like. Even for the short-run, "optimizing" choices cannot be made without a clear criterion, a standard of desirability. And the most significant criteria by which to judge a given command system derive ultimately from the national military objectives. If these objectives are sufficiently limited -- as is the first one we consider below -- a command system with little or no post-attack capability may be adequate or even desirable. The two objectives we discuss subsequently seem to demand a significant, survivable post-attack capability.

"DETERRENCE ONLY"

Much current discussion of command and control matters shows a relative lack of concern with post-attack problems; but this is not a matter of simple neglect. It reflects, in large part, attitudes toward the nature of thermonuclear war and towards desirable or feasible US strategic objectives that are, in fact, hostile to any marked increase in attention to post-attack control problems. In other words, there are certain obstacles -- in the form of beliefs and attitude -- even to a major research effort in this area. It would be important to the success of any such effort to confront these attitude-obstacles frankly and fairly

at the outset.

There seem strong grounds, to be discussed, for the belief that some form of post-attack control is highly desirable as an objective, and that research effort toward establishing its feasibility would be well spent. But rather than take these matters simply for granted, let us examine some contrary points of view which are widely held and influential, postponing for the moment discussion of the view of strategic objectives with which they are associated. Over-all criticism of these attitudes will be implicit in the arguments for post-attack control presented in the next sections, and may wait till then. However, some brief, non-definitive comments will be included in brackets along with each of the attitudes discussed.

(1) Post-attack control will never be used, since general war is, for practical purposes, impossible. Major nuclear war is so unlikely that a large expenditure of research effort on wartime problems is unjustified. This attitude, only occasionally explicit, is reflected in the nature of much current planning and procedures. Note that it implies: it is irrelevant what the plans and provisions for war actually are, so long as they promise to look frightening to the enemy.

[The notion that major nuclear was is virtually impossible seems dangerously invalid when applied to the present, and even more so for research directed toward 1965-1970. No one can pretend to estimate precisely the risks of war in that period; it would be exceedingly dangerous to prepare now on the assumption that they will be close to zero.][1]

(2) Post-attack control is unnecessary, because general war is essentially a simple affair. The circumstances that initiate major nuclear

war are simple, well-defined, predictable, and easy to recognize; there is essentially but one, at most two, appropriate responses, and these may be preplanned in detail (allowing for variations in alert, deployment, time of day, etc.). In theory, the later phases of the war might be hard to preplan; but in practice, no significant forces are likely to last past the initial preplanned exchange, anyway. They would have nothing very significant to accomplish if they did, since the initial exchange will be decisive.

According to this view, there will be nothing very important to decide during the war, provided that there has been adequate preplanning. The only important post-attack decision is the choice of preplanned response; and under the circumstances this is not regarded as a job requiring outstanding insight. In fact, many holding this view might be willing to see this choice made in decentralized fashion, if warning or bomb-alarm information could be disseminated reliably enough; but given the probable danger of false alarms, they tend to prefer that this decision -- and this alone -- be made centrally, for purposes of accident-prevention and coordinated action.

[We will comment at length on the notion of the predictable, preplannable general war in the next section; it appears quite unreliable. Briefly: we have never had a thermonuclear war; if one should come, there is every reason to anticipate that important aspects of it will not have been anticipated, nor appropriate responses preplanned.][2]

(3) Post-attack control is infeasible. Although data-flows could be speeded up greatly relative to past standards, holders of this view question whether lags could ever be cut enough to facilitate high-level control,

given their view of the tempo of nuclear operations. In fact, they raise this question in connection even with limited nuclear wars. They tend to worry that attempts by a high-level commander to "interfere" in ongoing operations during a major nuclear war would actually be detrimental; his decisions would be obsolete and irrelevant when he made them, and still more so when they arrived at subordinate units.

This argument affects particularly centralized, high-level control. But the problems of vulnerability of commanders and communications are regarded as even more intractable, and these affect every level of command, implying total infeasibility of prolonged control.

[We will discuss feasibility further in the final section. However, the attitude expressed above may exaggerate both the problem of tempo (particularly for later periods, when forces may be much less vulnerable on both sides) and the complexity of the hardware and the data needed for adequate post-attack control; it may underestimate, on the basis of inadequate research, the possibilities for providing a relatively austere but non-zero capability, and the incentives for doing so. Estimates of "feasibility" often tend, to a surprising degree, to be related to notions of desirability; we will consider the latter below, in this and the following section.]

(4) Post-attack control would be ineffective. Even if it could be achieved, even if war did occur, even if the war were not simple or predictable, continuing post-attack control could not significantly improve the outcome.

One basis for this view stresses the vulnerability and inflexibility of the forces commanded, allowing little scope for alternative employments (this is often a short-term view, looking at current forces). Another

emphasizes the inexorable, unmanageable dynamics of a major nuclear exchange, the ultimate tactics and outcome being independent of any early attempts at control. A third assumes enemy posture and tactics which would nullify any contribution of post-attack control.

The following section suggests several possible contributions that a capability for prolonged control might make to international stability and to an improved war outcome if deterrence should fail. But, under the present heading, it is possible to deny for varying reasons the feasibility or the net worth of each of these contributions.

[There is no doubt that questions of feasibility and effectiveness must tend to dominate discussion of short-run command and control problems: current "fixes" and systems planned, say, for the early '60's. Even for this period, however, there is reason to suspect that a thorough feasibility analysis will not reveal so black a picture as some critics suggest. For one thing, such critics seem to take little account of the various different circumstances under which war might begin. Also, they may overestimate the cost and complexities of a useful post-attack control capability; and weapons soon arriving may be capable of greater flexibility and lower vulnerability than current forces. Finally, the choices made by the enemy on posture and tactics cannot be so certain, and may not be so ominous, as these critics assume. However, these questions deserve attention and research; we will discuss them further in the final section.][3]

(5) Post-attack control would cost too much. This argument may be closely related to the above attitudes. It can be just another way of saying that post-attack control would never be used, or is unnecessary, infeasible, or ineffective. On the other hand, this view may concede

some degree of feasibility and effectiveness but stress the unacceptability of its expense. Three assumptions are usually made:

- o The military budget is essentially fixed, for political or economic reasons (i.e., the voters, or the economy, can't stand a higher military budget).
- o A post-attack control capability would be highly expensive.
- o Within the given military budget, other uses for this money are more important.

[All three of these assumptions may be questioned. Political or economic arguments that the military budget must be fixed are highly dubious even for the short-run; and looking toward 1965-1970, intervening crises could double or triple that budget. Moreover, there is little evidence now for (or against) the estimate that a useful post-attack capability must be highly expensive. Current proposals for elaborate surveillance, warning and reporting systems offer little basis for comparison; the capabilities may have little in common. Reliable cost-effectiveness research on this problem can scarcely have been done. (This also bears on the arms race argument.) Finally, in comparison with certain other components of proposed military budgets (possibly some aspects of these peacetime Command Control Systems) research or procurement directed toward a post-attack control capability can easily appear more rewarding.][3]

(6) Post-attack control would weaken the deterrent threat. There are several forms of this belief:

- o An investment in post-attack control capability would mean less resources for retaliatory forces. (This is another aspect of the beliefs in high expense and fixed military budget.)
- o An attempt to achieve flexible, adaptive, feedback control would slow responses and thereby increase vulnerability of

forces. (Mainly, though not entirely, a short-run view based upon current forces.)

- o By creating the prospect that some part of the surviving force might not be used in immediate, all-out retaliation against population (to be used instead against military targets or withheld as a controlled reserve), the mere existence of a survivable control capability might lessen the expected costs to the Russians of a surprise attack. Moreover, it might hold out the hope that Russian blackmail tactics could be effective, further improving the Russian prospects.

The fear that continuing post-attack flexibility and control might involve risks to deterrence suggests that such a capability is actually undesirable. It implies that only the prospect of an uncontrolled, automatic employment of the surviving offensive force can be deterrent.

[This argument seems to assume that the US force which the Russians would expect to survive their attack is so small, it would deter them only if the Soviets were certain it would be used entirely and immediately against their cities and population. But is this not a way of saying that the surviving force in question is too small? Surely it would be preferable to guarantee to the Russians that their attack would leave the United States with a surviving force whose capabilities are "frightening" even if they are not certain how it will be used: a second-strike force large enough that even the prospect of its controlled, calculated employment would deter attack. With such a deterrent force, we would not need to go to reckless lengths -- such as deliberately foregoing any attempt to achieve post-attack control capability -- to convince the Russians that we would surely use our force in the precise way that would be worst for them. Confronting the Russians with a whole spectrum of possible, unpleasant responses, we could free our hands to use the force, if war

came, in one of the ways that seemed best for us.]

(7) Post-attack control is provocative. Even the attempt to establish a wartime control capability suggests concern with the problems of war, an expectation that war might actually occur, a desire to improve the outcome of war and a possible belief that this could be achieved. All these might raise the enemy's expectations that the United States might strike first pre-emptively on a false alarm, or even preventively (since most control measures that would be valuable in retaliation could be even more rewarding in the context of a US first strike). This gives him an incentive to strike first himself.

Moreover, assuming that this control capability would be highly expensive and would necessitate a higher military budget, it might add fuel to the arms race.

[See the preceding comment under (6). A similar argument applies to the notion that a post-attack control capability (or a modest program of civil defense, or active defense, or counterforce capability) would be dangerously "provocative." That, too, suggests that the Russian decision to strike first is more delicately balanced than it "ought" to be, if our retaliatory forces were adequate. In other words, if a moderate, (conservative) attempt to alleviate the consequences of a possible war is all it takes to tilt the Russian choice toward "Strike," there is something very wrong with our deterrent capability. It would be a matter for great concern; the least we should aim for is an international order more stable than that.]

These seven attitudes are to some extent independent; it is possible to hold one while denying the rest. But in practice they reinforce each

other, and many critics seem to hold them all (whether they are consistent or not). It is significant to observe that many of these critics would hold similar positions if the phrase "post-attack control" in the headings were replaced by "counterforce capability," "active defense," or "civil defense." This is no coincidence. Together, all these attitudes and beliefs are associated with the coherent position: So far as major nuclear war is concerned, deterrence -- based upon assurance of retaliation -- is all that matters. This might be called the "deterrence only" estimate of US national strategic objectives. Other possible strategic objectives, such as improving war outcome if deterrence fails, are dismissed as infeasible, too costly, or destabilizing. Along with this restricted view of strategic objectives goes recognition of what Herman Kahn of the RAND staff has called the "spasm war" -- the spastic, uncontrolled, total expenditure of forces in a mutual paroxysm of destruction -- as an acceptable or inescapable pattern for major nuclear war..

Given these attitudes, whatever their basis, a preoccupation with pre-attack problems of command and control would appear thoroughly justified. To satisfy an objective of "deterrence only," a capability for survivable, prolonged, flexible post-attack control is almost surely dispensable, possibly even undesirable, whether or not it is feasible.

The attitudes above have been shown entirely in terms of their negative implications for survivable, flexible post-attack control; but they also have positive implications for system design. At least, they are compatible with the following system characteristics:

(a) Commitment (for deterrent purposes) to a single, all-out retaliatory strategy;

(b) High speed and automaticity of retaliation;

(c) Decentralized modes of response (to reduce vulnerability and hasten retaliation);

(d) Minimization of the role of human decision-making in favor of automated systems;

(e) Total reliance upon preplanning, preselected indicators, predetermined alerting and response procedures, predetermined commitment and decision rules.

The major function of a commander in such a system would be to enhance deterrence, on the basis of pre-hostilities posture and planning; he must, moreover, prevent accidents in peacetime and conduct cold war and "small" limited war operations. Large "Command Control Systems" might be needed for supporting pre-hostilities warning, surveillance and reporting functions, assisting in evaluation, planning and control. But their survivability under attack would not be an issue. If major nuclear war commences, the commander's last essential job is to push the appropriate button: if he has not arranged, through a bomb-alarm system and predetermined decision rules, that the enemy should push this for him automatically. Subsequently keeping him alive and in communication, and supplying him with information, might be planned for sentimental reasons or for marginal advantages in later phases of the war, but these would not be matters of urgency.

These views have been put in extreme form; and even among those who would accept them as stated, there are few who would argue that this approach represents an ideal way to fight a war. They would tend to emphasize feasibility limitations, the irreversible changes that have taken place in the nature of warfare, and the necessity to restrict US strategic objectives to "deterrence only." This last point is critical. If we accept the inevitability of the "spasm" pattern of war and the notion that the only feasible or desirable military objective with respect

to major war is simple, all-out, punitive retaliation, then a "collapsible" command structure of the above sort appears perfectly adequate. But is it, in fact, enough? It is not hard to establish that such a command structure, in itself, fixes very great constraints indeed upon the behaviors possible to the military organization, and the objectives which that organization may serve. Other behaviors and objectives may have seemed undesirable or otherwise unattainable, and thus, small loss, at the time such a command system was installed; but even if tastes or conditions should change, they will remain out of reach so long as that command structure persists. It will make them unattainable, whether they are so for other reasons or not. It is, then, highly important to know just what we may be giving up when we adopt such a system.

The most significant limitations of an "automatic response" system appear when we consider US objectives and strategies more complex than immediate, all-out retaliatory punishment of an aggressor. These other objectives might be discussed under two headings: "stability" and "improved war outcome." Both of them take for granted the prior objective, deterring premeditated attack by a calculating enemy; but they look beyond it. Both imply command and control requirements for survivability, flexibility and adaptability; they have, moreover, some implications for the desirability of centralized control.

Questions of feasibility and effectiveness will remain highly pertinent; we will discuss these at greater length in a final section. What the discussion above has tried to indicate is that the relative underemphasis on wartime control capability in current discussion of command and control is not typically a mere oversight, to be corrected by a casual

reminder. In large part it is a logical, explicit consequence of some strongly-held beliefs about the nature of thermonuclear war and the probable role of command decision-making in such a war. These beliefs may be right or wrong; but in general they are not clearly unreasonable, nor are they easy to disprove. It is against this context that we must proceed to examine the case in favor of a survivable, flexible post-attack control capability: the strategic objectives of stability and improved war outcome.

"STABILITY"

War can begin for reasons other than the premeditated act of a rational opponent. Events can take place, unchosen, which increase the likelihood of a major nuclear war desired, prior to those events, by neither major participant. To pursue "stability" is to attempt to lower the likelihood of war, (a) by making such "destabilizing" events less likely, and (b) by lessening their destabilizing effects. A command capability which would retain flexible control under attack would contribute to stability under several sorts of circumstances.

(1) It can reduce the chance of an accidental discharge of a nuclear warhead or an irrational, unauthorized or mistaken action by a subordinate leading to such discharge.

The contribution here may be somewhat indirect, but still important. Strictly speaking, there is no doubt that measures are possible which could greatly reduce the likelihood of such events even without creating a survivable, post-attack control system. But there are reasons why such measures are considerably less likely to be taken in the absence of such a system.

When the command system itself is highly vulnerable to surprise attack, there are bound to be strong, though perhaps unspoken, pressures against any measures which would attempt to make "unauthorized" action by subordinates strictly impossible. This is particularly true when the offensive forces themselves are vulnerable and rely for their survival and effectiveness upon fast response. The real possibility that headquarters down to relatively subordinate levels might be destroyed even before they could issue or pass on an "Execute" order implies that a retaliatory force in which "positive control" was absolute might be totally paralyzed by a blow at its nervous system. At the least, it might be so slowed in its response that its weapons systems could be destroyed by the attacker with much higher confidence.

Short of reducing the vulnerability of the command structure, there may appear two paths of escape from this nightmare. The first is to abandon the positive control principle -- which permits the execution of nuclear strikes only upon the positive, authenticated order of the highest command -- by authorizing decentralized action under certain circumstances: e.g., given outage of communications and/or other evidence of destruction of higher headquarters.

In certain forms, a back-up, decentralized mode of operation may well deserve consideration. There is always the possibility that centralized facilities, no matter how well protected, may be destroyed; and research might discover decentralized modes that would look preferable in such event to having the system "fail dead." The problem is that there will usually be some ambiguity in the evidence available to the subordinate unit as to whether the time has come for it to exercise its authority,

Continued →

i.e., as to whether or not the higher headquarters has been destroyed by major nuclear attack. The most careful schemes would take great pains to reduce this ambiguity so far as possible, by providing bomb-alarm systems and positive means of interrogating higher headquarters; but proposals have been made which give scant attention to such safety measures. The "softer" the command and communications systems -- the more vulnerable they are to natural disasters, to a single nuclear explosion (which could be an accident on either side) or to a small number of explosions (which could result from enemy unauthorized action) -- the more ambiguous is such an indication as outage of communications with headquarters. And the more ambiguous this evidence, the more likely that, out of hundreds of subordinate units, some one unit will experience someday a false alarm that decides it to "Go."

The other escape path is even less easy to control and may be much more accident-prone. That is to retain "positve control" in principle, but to allow attitudes and practices to develop which undermine it in practice. In effect, this approach relies upon unauthorized action to provide assurance of retaliation, in case command centers are destroyed. This policy is unlikely to be explicit, or even wholly conscious; it shows itself not in direct encouragement of unauthorized action, but in acceptance of the possibility (and value) of such "initiative" under attack and in reluctance to adopt measures which would render it highly difficult. (Such measures might be symbolized by the combination lock on every nuclear weapon: the "Execute" order supplying the combination.)

This "solution," being wholly informal, will be less subject to careful analysis and criticism either on grounds of reliability or safety. It can lead to the worst of both worlds: a system which is not very likely to

14M ≒ C-II

Go when an attack has really occurred, and which is excessively likely to Go (at least in part) when an attack has not occurred. Since no unit is explicitly authorized to execute war plans without positive order, no great effort will be made to provide subordinate units with reliable, unambiguous evidence that a major attack has taken place or that higher headquarters have been destroyed; hence, if an attack does take place, few units which are not themselves struck initially may get evidence sufficiently unambiguous to tempt them to initiate attion. But in an atmosphere sympathetic to "initiative," even highly ambiguous -- and false -- evidence of attack may prompt some one individual, group leader or subordinate commander, to take irrevocable action in the national interest as he sees it. And his capability to respond to that "challenge" might be very great, given a general hostility beforehand to measures highly likely to frustrate it.

In contrast to these approaches, the provision of a protected, survivable command and communications structure would give reassurance that the issuance of an authenticated "Execute" message, could not easily be blocked by a paralyzing blow at the central nervous system. A strict, "positive control" system would no longer appear to entail such risks to the reliability of a retaliatory response; there should no longer be pressure to abandon or circumvent it, or resistance to measures aimed at making it more effective. There might still be interest in designing efficient, decentralized back-up modes to ensure against the possible failure of the protected, central command system. But there would not be the temptation to adopt desperate and poorly-analyzed measures, dangerous "quick fixes" or tacit approval of "unauthorized" action, as

At the outset of an unwanted war, not all the surprises need be nasty ones. Imagine, for example: an unexpected interval of reliable warning; a thoroughly bungled Soviet attack, a windfall of information on military target locations; prompt willingness of Soviet leaders -- perhaps newly "appointed" ones -- to capitulate after the earliest exchange. But even these relatively pleasant surprises would quickly turn bitter if it were impossible to exploit them because of the rigidity of our plans or the early failure of our command and control system.

Of the four classes of surprise mentioned above, the last two are often neglected: the reactions of decision-makers in a crisis, and the response of the organization to command. With reference to the first, decision-makers may be confident during the planning process that they can predict the responses they would wish to choose in a given contingency. They may be wrong. When the challenge actually confronts them, they may suddenly perceive previously-unnoticed merits in unplanned ways of acting, and defects in the planned ways. They may discover paralyzing ambiguities in signals that were planned to trigger action, or urgent significance in cues no one had planned to look for. They may invent and follow wholly new ways of acting.

To a computer enthusiast, this unpredictability may be despicable; and if it were due entirely to human failure under stress, to hysterical panic or fatigue, it would indeed be testimony to the unreliability of human components and an argument for the prior automating of the system. But in fact, many of these new responses might be the more valid ones. They may simply reflect the fact that the decision-maker is now taking this situation seriously. Certain types of consideration which influenced him importantly during planning (e.g., political or budgetary) may suddenly,

C-II

Taiwan Straits

C-I

urgent insurance against the all-too-likely failure of an unprotected system.

(2) No matter what precautions are taken to ensure "positive control," the chance of an eventual accidental discharge, unauthorized, irrational or mistaken nuclear commitment on one side or the other is not likely to fall to zero. If the nature of this event, having occurred, were recognized by one side and could be communicated convincingly to the other (which seems just possible, especially with some prior preparation for such a possibility), both sides would have an interest in limiting the exchange. Preparations might involve contingency plans, and special information/communication/demonstration/inspection capabilities. Such an attempt could probably not be "high confidence," and no doubt many conditions would have to be fulfilled before it could become even promising. But one precondition would be: the command system of the nation suffering the nuclear explosions must survive them.

More dangerous than a single nuclear accident would seem to be the deliberate, unauthorized action by a subordinate, which raises the possibility of several, well-placed explosions directed at the opponent's main headquarters, his centers of military and governmental authority. Suppose that the victim's command and communication system were such as to collapse under these few blows, with assurance of retaliation provided by a decentralized back-up mode. The chance to contain such a war might be very small in any case; but such a collapsible command system would totally foreclose it. The likelihood of this contingency might seem low, but hardly low enough to ignore. We cannot be absolutely certain of the effectiveness of our own positive control system; what assurances have we that the Russian system is even as good? Should we guarantee that the

unauthorized action of a fanatic Russian squadron commander must, without fail, trigger "war to the finish"?

(3) The above problem is with us now. But a similar one will arise even more inescapably in a later period when a number of nations might have the capability for sizable nuclear attack, perhaps from submarines, concealing the nation of origin. In that era, the chances of accidents or unauthorized action might also be much greater. These considerations alone create a requirement for a control system with broad access to varied information, capable of identifying an attacker and of making a deliberate, appropriate, non-automatic response; and, for these purposes, capable of surviving the initial attack. This, incidentally, is a problem for which the decentralized back-up mode would seem to provide no answer.

(4) If, as is generally assumed, both sides proceed to acquire large and well-protected "second strike" forces, then either side might be less restrained from "expanding" a limited war by the fear of provoking an all-out attack from the opponent.[2] In this case, exchanges might occur which were extremely "large" by present concepts of limited war. In the extreme -- if the ultimate balance of terror were very stable indeed -- these might approach "limited general war," featuring limited attacks upon the opposing homelands and strategic forces. The plausibility of the latter situation is highly controversial: as is the notion that we would ever be concerned to "stabilize" a conflict presenting a deliberate attack upon Washington or SAC Headquarters. But wars far short of that, wars which the United States might strongly wish to regard as limited, could feature nuclear attacks upon lesser command posts and communications: for example, in the theaters. This will be true particularly when more nations -- such as

Communist China -- acquire nuclear weapons (and we may not be aware precisely when that era has arrived).

We have already noted that it may be misleading to assume that such attacks will be confined to general war, whether that term is understood to mean all-out conflict or simply war with Russia. To say that such attack would inevitably "constitute" general war or "should" lead to a a general war response amounts to saying that the United States would surely want to launch all-out attacks on Russia if the Chinese Communists, in the course of a limited war, should drop a bomb on CINCPAC Headquarters, or even if the CHICOMS should unexpectedly blackout HF communications in the Pacific.

Yet given a theater command structure highly vulnerable to attack, even inadvertent or unauthorized attacks upon command centers or communications during a limited war are highly likely to lead to automatic expansion to general war on the basis of preplanned responses, though neither side might have foreseen or desired this result. "Collapsible" command posts and communications in the theaters can be as great a threat to stability as similar systems in the homeland.

Assuming, for purposes of this discussion, that high-level command posts in the homeland may be considered sacrosanct in even the largest "limited" war in the future, the solutions to this problem might be: (a) making communications from central command posts to all nuclear strike forces highly reliable and invulnerable, so that the homeland is assured of residual control if theater command posts or communications are disrupted (avoiding schemes for decentralized action by theater forces); and/or (b) hardening theater command facilities and communications (a start might be to protect them against HE attack).

IMPROVED WAR OUTCOME

Whereas the goals of "deterrence" and "stability" have to do with reducing the likelihood of major nuclear wars -- both premeditated and non-premeditated -- the goal of "improved war outcome" assumes some likelihood that major war may commence despite these basic policies. It affirms the desirability of alleviating the civil and/or the military and political consequences of such wars as do occur.

This will involve some measures that are largely passive, such as fallout protection and relocation of strategic bases away from population centers. But it will also call for an active capability in such wars to govern our behavior in terms of "what is best for the United States" as opposed to merely "what is worst for the enemy." The latter might be much easier to pre-program unconditionally; the former may call for the ability to perceive, transmit, interpret and respond flexibly to rapidly changing information, much of it unanticipated. Improving the war outcome will involve limiting damage to the United States and its allies; conducting hostilities in a manner designed to serve US interests; and achieving an end to the war, with military victory or stalemate, on terms advantageous compared to the results of an uncontrolled exchange.

Such goals place requirements upon weapons systems, force structure, active and passive defense, contingency war planning and tactics; and their achievement will also depend critically upon enemy posture and tactics and the circumstances of war-initiation. What concerns us here is their requirements for information flows, command structure and communications. We will consider in turn requirements for counterforce capability, for threat-strategies, for flexible, adaptive behavior, and for responsible

military/political direction. These seem to demand such characteristics in the command system, beyond survivability, as a high degree of coordination, substantial post-attack information flows and data processing capability, and possibly centralized direction in certain functions.

(1) Counterforce capability. There is more than a possibility that significant fractions of the offensive forces of both sides will continue, in the near future as in the recent past, to be highly vulnerable to offensive action by their opponent. This condition might persist much longer than is now commonly assumed. To be sure, it seems likely now that both sides could take measures in the coming decade to preclude this situation; but some past experience suggests that, in fact, they might not take those measures. So long as the Russians do not, the United States might have a great stake in an ability to exploit the vulnerability of enemy forces, either in a US pre-emptive strike or striking second. The United States might thereby hope to improve the outcome of a war in two ways: by directly limiting the enemy's ability to inflict damage; and by improving the post-attack balance of forces, thus supporting US threat-strategies and influencing favorably the outcome of the war.[3]

Surely we should be alert to the possibility or likelihood of significant changes in strategic posture: and these might rule out counterforce as an important capability. But at the same time, we should by no means discount to zero the likelihood that systems of 1965-1970 will still have important resemblances to current systems, even in what we consider current faults. It is risky to estimate future postures entirely in terms of technical feasibility and "rational" considerations. Current postures on both sides could not have been predicted accurately on such a basis. Indeed, an examination of the peculiarities of current posture on

both sides should be a reminder of the richness of future possibilities, and in particular of the importance of inertia, cross-purposes, faulty analysis, lack of calculation, and totally unforeseen developments.

This is not to say that a counterforce capability can be pursued with high confidence that it will prove effective; at most, it is an argument against foreclosing possibilities. If it should otherwise prove feasible and useful, it would almost surely require continuing, post-attack direction capable of fast, flexible response adaptive to rapid information inputs. Many aspects of these operations might well be highly decentralized; assuring their survival is nonetheless part of the task we have called "protecting a post-attack control capability."

A major counterforce capability is not the only way to improve war outcome, so its lack of feasibility would not rule out that goal, nor would it markedly affect the case for post-attack control. However, many estimates of its feasibility in current popular debate in the public press seem excessively pessimistic.

A case can be made that there will continue to be important military targets of fixed location in Russia in the 'Sixties, and that we may know the location of many of them. Thus, US decision-makers might have a significant choice of target systems to hit, on receiving indications of an attack: <u>if</u> they stayed alive and in control, and if their plans and vehicles were flexible enough.

To say that a case can be made for such counterforce possibilities is not to say that it has yet been made, in reliable fashion, any more than the opposite position has been thoroughly established. There are surely enough grounds for interest to justify research: and to be wary of foreclosing the issues by adopting a collapsible, one-shot command system incapable of adapting to the precise circumstances of the war or

of exercising the feedback control probably needed (at some level) for conducting counterforce operations.

(2) Threat-strategies. One of the most powerful hopes of achieving such objectives as limiting damage to the United States, compelling surrender or avoiding military defeat, and ending the war on acceptable terms would be through the employment of strategic threats, based upon retained forces. In fact, if the world predicted by the pessimistic critics of counterforce capabilities should come to pass, one in which our opponents possessed large, essentially invulnerable retaliatory forces, these might be the only hope of achieving such objectives.[3],[6]

Assuming that it is impossible wholly to disarm the opponent by direct military means, threats of the use of surviving, retained forces against remaining enemy targets might induce him to hold back his remaining force, or at the least, to restrain its employment (e.g., to avoid US cities). Since it would be necessary to preserve conditionally enemy targets to be threatened, reliance on this tactic would not be consistent with an immediate, all-out retaliation against cities; but if the assured, second-strike capability were large enough, this restraint should not jeopardize deterrence.

This particular strategy would seem to require a survivable centralized political and military control of forces, with the ability to withhold reserve forces on which threats may be based, to make limited "demonstrations," and to communicate authoritatively with enemy leaders. This might conflict with a decentralized conduct of counterforce operations; it might be important for a central "bargaining" agent to be able to redirect counterforce missions away from important population targets, constrain them,

stop them, or use them for "demonstrations" of the ability to carry out threats.

Like counterforce, this strategy will provoke skeptical questions: "Is it really credible that such 'threats' would influence Soviet leaders, in the heat of nuclear war? How would we convince them of what we had left? Would Soviet leaders still be alive, and in control of their forces, after the initial exchange? Should we deliberately avoid their control system in our retaliation or first strike; and even if we did, would their control system permit them enough leeway to control their operations effectively in accordance with our threats? Would the Soviets avoid our cities in their first strike?"

These questions are important and deserve investigation. However, skepticism at this point would seem to be even more premature than with respect to counterforce. Even less research on the real possibilities has been done; and it seems hard to make a case that there is much to lose by preparing to implement such tactics.

Even if we were to accept the premise, unfavorable to counterforce, that there would be no military targets of known location to hit, the conclusion would not follow that expending all our forces immediately upon cities was an optimal initial response. It would be absurd to accept as conclusive the rhetorical question, "What else is there to hit?" It is not uncommon for a deerhunter to pick off a bystander in the woods; but he does not seek to explain this, "There was nothing else to hit." If counterforce is ruled out, neither deterrence nor any other US objective demands that <u>anything</u> be hit <u>immediately</u>. If some part of the force can survive for hours or days, a decision-maker could determine, at least,

the time-pattern of its use: if he survived, and could control it. He could then use it rationally to support threats, to counterbalance the remaining Russian force, to influence the Russian conduct of the war, to bring them to terms. Even a slight chance that this use would be effective could make this strategy seem preferable to an uncontrolled exchange.

We have already noted that the prospect of a sufficiently large "strike second" military capability -- even if it were controlled, even if it were planned to be devoted to counterforce and threat strategies -- need not jeopardize deterrence. Would the protection of a post-attack control capability, in itself, help deterrence? No position will be taken upon this point here. A surviving control capability might considerably increase the efficiency even of a punitive retaliatory strike against population; e.g., if it allowed retargeting; it would in effect, increase the size of the threatened retaliation. This might significantly improve deterrence if the post-attack force expected to survive were small to begin with. On the other hand, it would seem at least as important in that case to increase the protection of the force; and that done, the contribution of a retargeting capability to a retaliatory threat might be marginal.

However, the combination of threat-strategies and counterforce capability (to the extent feasible) might provide a new basis for deterrence which, if not actually more deterrent, might be much more satisfactory from other points of view. Even if the US force were substantially protected, some relative vulnerabilities would remain; an opponent, striking these, might hope to achieve a military advantage, an asymmetry in his favor of remaining military capability on both sides and of subsequent ability to pose military threats. If there were no response to this attack, or if

the response were directed only at population and cities, the attacker would have an advantage in any ensuing exchange of threats. This military "victory" might (or might not) be hollow; but given even a limited counter-force capability, the United States might not need to concede even this measure of success to the attacker. It could use this limited capability to cut the attacker's remaining military capability down to rough equality, eliminating (without necessarily being able to reverse) the asymmetric advantages achieved by his first strike.

This could be more plausible and no less compelling a deterrent than a threat against population. Given the probable military/political goals of the attacker, a plausible threat against his residual military capabilities might place in hostage something as precious to him as cities. And if deterrence failed for any reason, this strategy could provide rational employment for part of the force, serving as "demonstration" of continued control and resolve, increasing the relative significance of withheld forces and hence the effectiveness of threats based upon them.

The feasibility of either counterforce or threat strategies depends critically upon the nature of the surviving, post-attack control capability. They constitute two rather specific ways for improving the outcome of a war. But arguments remain to be made for a survivable control capability which do not depend upon an optimistic estimate of any such specific tactics. In the next two points, we shall consider some broader characteristics of behavior designed to achieve "what is best for the US" during a war, along with their implications for command and control systems.

(3) Flexible, adaptive behavior. A good deal of "flexibility" and quasi-adaptive behavior can be preprogrammed. To the extent that contingencies

with different implications for desirable behavior can be anticipated, and the appropriate responses calculated in advance, an "automated" system can be responsive to varied and changing circumstances. A library of contingency plans can be drawn up, an automatic information network for perceiving and transmitting the relevant, preselected indications set up, and decision rules assigned to appropriate units for the selection of contingency plans relative to indications. This system can be designed to operate only at the start of hostilities, responding to the circumstances of war initiation but lacking the capability to survive or further influence operations. Or it might conceivably be programmed to continue to process preselected types of information and to modify operational behavior during hostilities.

A well-recognized constraint upon the complexity of such preprogrammed behavior is the limited capacity prior to hostilities to generate many relevant contingency plans. A major contribution of electronic data-processing systems may be to increase this capacity, permitting a richer variety of prehostilities contingency plans. Such plans, plus prehostilities effort to discover relevant indications and their implications for policy, are beyond question essential; prehostilities preparation can and must cut down the decision-maker's wartime tasks to manageable size.

The question is whether the "decision-maker's" role can be entirely eliminated during wartime. Some enthusiastic treatments of the possibilities for preprogramming would almost imply that it can: that a properly preplanned response mechanism need leave no room for "command decision." Their preferred "man-machine system" would stress the "machine" role during wartime much more than that of "man." Human decision-making would be dominant in peacetime, in the design of the system and the choice of contingency plans. But during wartime the speed and capacity of the computer

coupled to an automated data-transmission system, with its relative freedom from environmental stresses, fatigue, anxiety or panic, its specialized precision and reliability, would make it, in this point of view, the preferred component compared to man. (Vulnerability aspects, among others, tend to be slighted.)

But enthusiasts for "dehumanized" response schemes typically neglect another constraint upon the effectiveness of the totally preprogrammed system; the ability to foresee relevant contingencies and desired responses. The general problem here is that of dealing with surprise: with information, events, evaluations which were unanticipated in the programming phase, and for which no plans exist. What is most interesting here is not the occurrence of an event which was considered "unlikely" and for which inadequate provision was made: but the possibility of happenings which were considered "impossible" or were undreamt-of, to which the plans gave no attention and which find the victim without insurance. A system which relies totally upon the automated selection and execution of predetermined plans is, virtually by definition, unequipped to respond appropriately to surprises.

What is the likelihood of such surprise? Planners tend to deprecate it. Yet it is not hard to find historical examples, particularly in the initial phase of hostilities, the interface of peace and war. Here is where the peacetime concepts, plans, posture and expectations meet their first test: and often fail. Of innumerable cases, two are particularly striking (ignoring, in both, the "tactical surprise" in terms of timing): the capabilities and daring exhibited by the Japanese in the Pearl Harbor attack; and the location, tactics and, above all, tempo of the German

armored push through France.

One privileged to examine war plans in any given period might, perhaps, find that they ignore certain plausible contingencies. What general conclusions should one draw about such gaps in the plans? Some would regard them primarily as specific shortcomings of the particular planning process involved; the cure is to fire the old planners, design new planning processes, fill the specific gaps discovered and be more careful and imaginative in future. To some extent this is a reasonable reaction. It is a function of a planning process to prevent or minimize surprise; and new tools and methods (e.g., war gaming, simulation, systems analysis, more varied contingency planning with the aid of planning models and electronic data-processing systems) offer hope of improving on the historical record. But is it reasonable to expect that important surprises will be eliminated? Is this even a reasonable aim?

A closer examination of past surprises and current potential surprises will find causes for many of them of a sort most likely to persist in the future, no matter what the elaboration in the planning process and information structure. This is to say, there will continue to be surprises.

Potential surprises may be categorized in different ways, but we might draw attention here to four classes in particular: (a) enemy threat, in terms of capabilities, posture, doctrine, objectives, tactics; (b) political and military environment, including technological developments and changes in alliances and allied capabilities and policies; (c) the central decision-maker's interpretation of given signals, perception of available actions and their relevant consequences, evaluation of alternatives, at the moment of decision; (d) the actual performance of the organization in carrying

Map 1
C-II

out a given decision. If we accept the premise that important surprises may occur in each of these categories, despite all prior efforts to anticipate significant possibilities, we must be interested in the capability of the organization to adapt its behavior to events in ways that cannot be entirely preprogrammed. To adjust to surprises, the command and control system must be able to survive them and perceive them, to recognize them as surprises relative to previous expectations and plans, to re-evaluate alternative courses of action, to make and communicate decisions, to produce postures and operations different from any in pre-existing plans.

How much it is worth to achieve this ability will depend on one's estimate of the likelihood of major surprise. At this point in history, that estimate can be made with unusual confidence. One can state almost axiomatically: In the first thermonuclear war, surprises are to be expected.

There have been other periods when technology underwent major changes between one war and the next; but in most cases, the planners in the transition period were blissfully unself-conscious about the possible implications of those changes, and they went into the ensuing war clutching their plans with assurance, confident they knew how it was all going to turn out. We have no excuse for such blindness. Suppose that we look only at our current opponent, current technology and the prospects for the next few years. Rarely has one faced an enemy so secretive; rarely have his weapons, tactics, men -- and one's own -- been so untried; never has the quantum jump from the weapons and strategies of one war to those of the next been greater. Looking ahead, at the unprecedented rush of changes in technology, the possibilities for the dispersion of advanced technology and changes in the roll-call of alliances, the uncertainties seem still greater.

perhaps correctly, appear trivial. Risks which seemed unthinkable earlier may now appear clearly preferable to their alternatives; the same might be true of retreats. The detailed specifics of the situation will fully enter his calculations, perhaps really for the first time.

Thus we may have surprises of "command": and just so in "control." In principle, if the command and control system features feedback, "closed loop" control of operations, it is designed to detect "errors" in performance and to modify behavior to reduce them. In practice, even such a system may monitor only certain aspects of performance, and in those perceive only certain types of "errors." Wide deviations from operational objectives might be possible of a sort which the control system was not designed to notice or to correct. This might be more likely in the first realistic test of the system: particularly when the operational objectives set, the "command decisions" discussed above, themselves constitute "surprises" to subordinates.

Such problems are grossly magnified when the control system is essentially an "open-loop" system, lacking feedback of performance data and survivable capability for modifying behavior. Although the shortcomings of such a system are well known, its possible advantages in terms of speed of response and vulnerability have recommended it to some designers of a retaliatory response mechanism. In their proposed systems, a button is pushed (the command decision) and the system commits itself irrevocably. Minimum provision is made for monitoring actual performance, for requiring confirmation or acknowledgment of receipt or interpretation of messages; such extra loops would slow down response and would offer additional points for the enemy to cut circuits and disrupt retaliation. This leaves little opportunity for commanders even to <u>detect</u> "surprising" behavior in the

reactions of subordinates to their commands; and their capability to modify those reactions in time may be negligible.

There is another rationale for such a system that may be even more important, though unspoken. This goes back to the concept of "general war" as a simple, unambiguous sort of situation. By this attitude, the circumstances that lead to "general war" are perfectly well defined, the enemies are known, the objectives simple, unequivocal and constant, the courses of action easily laid out in advance. What room is there for error, misunderstanding? Once a decision has been reached to execute general war plans, who could be so stupid as to distort its simple contents in transmission or in interpretation?

Such an attitude, deprecating the likelihood of surprises in performance, not only encourages an open-loop control system, it magnifies its potential defects. The high speed of response in such a system is always somewhat suspect, since the question must arise of the appropriateness of the response. With decisions of such consequence, one would wish the utmost concern at each level of command that the planned implementing responses, at least, should be appropriate: the right messages sent or relayed, the right interpretation assured, the appropriate action planned. Yet the belief that inappropriate behavior is "unthinkable" is likely to create a casual approach to these critical problems. Given the difficulty of a fully realistic test of the system during peacetime, and the likelihood during war of "surprise" command decisions (never reflected in earlier exercises), very serious potential discrepancies can lurk unnoticed in the likely performance of the system. The control system designed to cope with "simple, predictable" thermonuclear war will be not only ill-equipped

to deal with surprise: but surprises will be built into it.

The capability for adapting to surprise is essentially related to the capacity for learning. Such techniques as war gaming, simulation, and field exercises may provide some "learning" before a war; they must be exploited to reduce the likelihood of surprise. Nevertheless, the first stages of a future conflict are sure to be devoted to surprises and to new learning, much of it hard and bitter. That is, the learning will take place if the parties have the will, the time and above all the capacity for it.

Conceivably one of the surprises of the first thermonuclear war may be that the tempo of initial stages is not so fast as we tend to expect. As in the Second World War, there could be initial periods of "phony war," abortive exchanges, or "test cases," providing a windfall of time and experience, if the command system were prepared to exploit it for learning. Barring such developments, the time for learning in a nuclear war would, no doubt, be very short. In the past, even at a slower pace and long duration of hostilities, it has usually taken all of one war to learn lessons that will be obsolete for the next. If learning processes must follow historical experience, it would be easy to be pessimistic about the prospects. But the need can be seen in advance more clearly and more urgently than before, and perhaps with enough will we can develop the capability.

What capabilities are required? Clearly, the requirements for information input during hostilities, for data-processing and transmission, for analysis and evaluation, will be much greater than would seem necessary if stereotyped perception and responses were believed to be adequate. These requirements may expand at many points in the military organization, for ideally learning could profitably take place at many levels of command.

But there may be peculiar requirements for centralized decision-making facilities, which can draw on the greatest variety of information and experience and which may, in fact, be specialized for learning.

In higher animals, the seat of learning is the brain. It is informed by memory, by sensory receptors reporting on the outside world, and by proprioceptive receptors that report on movements and processes of the body. The genes prescribe inherited reflexes, automatic responses to threats and challenges that have confronted generation after generation so that the species has developed appropriate stereotyped responses by processes of natural selection; this corresponds to "preplanning" and "decentralized execution." But the genes pass on another heritage that has proved vital for dealing with unfamiliar and transitory challenges: the design for a brain. [5] The brain controls processes of trial and error, observes the results, gradually improves the responses and stores acquired "learning" in memory. Thus it serves to keep its owner alive. It is worth emphasizing this last point, that the brain is not just a happy gift of Nature designed to make animals more interesting to other animals; it is, as W. Ashby has put it, "a specialized means of survival."[5] However, since learning takes time, the brain cannot counter threats to itself on their first appearance; hence evolution has housed the delicate learning apparatus in a "hardened," protective shelter.

Someday machines may have acquired some similar competence in managing processes of adaptation. Research is now being directed toward programming computers to utilize heuristic techniques in problem-solving and to exhibit aspects of "intelligence." But the day when they can compete with humans in such learning and problem-solving roles lies far

in the future. Here is an area where the human component in the system is indispensable.

Whether an organizational "brain" should, as in humans, be concentrated in a single, protected center is a matter for argument and research. The arguments for having such a center (supplemented and backed-up by subordinate centers) seem powerful, but they should not be taken for granted. In any case, however the functions of a brain may be distributed throughout the organization, it would seem highly important to assure the survival and post-attack of an effective learning capability, with its supporting information system. Curiously, many current military planners seem almost sanguine about the prospect of losing the military central nervous system and all its sensory inputs at the outset of conflict. It is as though they were planning to send a boxer into the ring, well equipped with a brain but lacking a skull.

(4) Responsible, political/military control. The question of centralized versus decentralized control of operations deserves much research. It need not be an all-or-nothing decision; probably research and analysis will show that certain processes and operations are best controlled in decentralized fashion, others in more highly coordinated fashion. But it seems inappropriate, in dealing with problems of thermonuclear war, to be entirely neutral toward these organizational modes, and in particular to deprecate the critical role of constituted authority or of the specific, highest centers of command.

There is every reason to preserve an attitude of awe toward megaton thermonuclear weapons: to regard control of their deliberate, calculated employment as an inescapable trust, not lightly to be delegated. "Conventional" though they may be in numbers and cost, they remain terrible

in consequence. If war is too serious a matter to be left to generals, thermonuclear war is surely too serious to be left to hundreds of isolated majors and captains to take over from the generals. Quite apart from the accident problem, it is anything but a light step to commit a single megaton weapon to the discretion of a subordinate, even in wartime, whether limited or general. It would be even more serious to commit ourselves so rigidly in advance of hostilities that our employment of such weapons is left, in effect, to the discretion of the enemy. These are desperate measures. If they should appear necessary in the 'Sixties, it will be for the total absence of alternatives.

A controlled response under enemy attack will be difficult. Conceivably it might, despite all efforts and ingenuity, come to seem impossible (at least in the worst cases). But surely military planners should not start with the assumption that control is unattainable, or disclaim responsibility for attempting to exert an intelligent, informed, calculated influence upon the course of hostilities. It would be irresponsible for a top military commander to plan to die at the outset of general war. He might equally well plan to resign in the face of battle. The military leader has no business planning to be absent -- or incommunicado -- the second day of the war.

Nor should he plan to lose his boss. It is his job to obey the political leaders of his country and their interpretation of the national interest, and to preserve their leadership. It is not their job to protect themselves; it is the job of the military to protect them, and their advisors, in the performance of their function.

Their function -- and their political experience -- may even play a more critical role in future conflicts than in past. For one thing, the

"threat-strategies" mentioned above do not rely purely, or even mainly, upon "military technique." They are aimed at the minds of enemy leaders; they depend for their effectiveness upon psychological and political expertise. For such tasks, possessors of political judgment, experience, and information have essential qualifications.

There is a more general consideration. The notion of "purely military" objectives or considerations has always been sterile and misleading at the strategic level, but never so obviously as in connection with an exchange of thermonuclear weapons. Quite aside from constitutional questions of authority, it is clear that the nation's political leadership, with their over-all view of national objectives, and their generalized sources of advice, information and experience, must play a central part in the conduct of major hostilities.

III

SOME COMMENTS ON REQUIREMENTS AND FEASIBILITY

Ideally, an integrated "war-fighting" (damage-limiting, war-ending, war-winning) capability would demand a highly survivable, coordinated command and control system, capable of both immediate and delayed responses, with monitoring and feedback control of operations. Some important functions would be centralized, under responsible political and military leadership. For purposes of stability, adaptation, and rational control, the system would be capable of receiving and processing significant amounts of intelligence, reconnaissance, surveillance and status data during hostilities with facilities for generating plans and communicating both with the forces and the enemy.

This is not to say that any of these functions would be preserved on a scale comparable to the pre-hostilities system. The facilities and amounts of data handled might be minimal compared to any but the zero capabilities of a "collapsible" system after attack. With this caveat, let us consider some specific capabilities that might be desirable:

1. Strict positive control of nuclear weapons, with maximum safeguards against accident, or unauthorized action, with weapons, communications and decision-makers sufficiently invulnerable to assure reliability of retaliatory system.

2. A bomb alarm system conveying fast and unambiguous indication of enemy attack, not only to command centers but to nuclear strike units (even if the latter are not, in fact, authorized to act on this evidence, demonstration of this system might deter attack on the command and communications systems).

3. Sufficient variety and amount of reconnaissance/surveillance/intelligence information to reduce the ambiguity of warning, lessen the likelihood of false alarm, and increase capability to identify the attacking nation; the ability to shift or augment rapidly the resources for gathering this information, both for pre-attack alerting and post-attack reporting.

5 3
3 6

8

4. The ability to preserve responsible political/military control of operations, preferably at the highest national level, with sufficient information input, communications and data-processing capability to permit not only a choice among contingency plans but some departure from existing plans.

5. The ability to discover and destroy a significant portion of remaining enemy forces.

6. The ability to discover rapidly the nature of enemy tactics, the effects of the enemy attack and the combat performance of the enemy and U.S. strategic forces; to perceive deviation from expected patterns; to "learn" rapidly from this information and to modify ongoing operations on the basis of this learning.

7. The ability to choose among different target systems and to modify this choice during hostilities, perhaps by retargeting alert missiles or planes in flight; individual, selective missile control.

8. The ability to support threat-strategies, to hold some forces in reserve and under flexible control with assurance of their survival, and to preserve enemy targets provisionally; the ability to transmit reliably not only "Go" orders but also "Wait," "Stop," "Shift," "Return," or "No" orders.

9. The ability to coordinate retaliatory forces supporting threats with ongoing counterforce operations (which may in some aspects be decentralized); the ability to monitor, redirect or stop counterforce as well as retaliatory missions.

10. The ability to communicate with enemy leaders, political and military, threatening the use of surviving forces held in reserve against previously unhit targets (this might even be used to cause them to abort an attack in its early stages, if reliable warning were achieved, or to contain an exchange begun by accident, unauthorized action, or false alarm).

11. The ability to give persuasive evidence of surviving military capabilities, to carry out "demonstrations," limited retaliation, and intra-war negotiation (if necessary, using cover and deception to exaggerate remaining capabilities for bargaining purposes).

12. Following successful threats or initial operations, the ability to receive from the enemy proposals of surrender of of ending hostilities, with information on his forces, status and operations, and assurances as to future activities; plus the ability promptly and reliably to check such information and assurances, by surveillance, inspection or direct control.

Critics may say that such a list of capabilities is asking for the moon. It is rather like the moon; it looks far off, but we might be sorry if the Russians get there first.

This by no means implies that feasibility and effectiveness questions are to be dismissed. On the contrary, they must be at the core of a research program addressed to command and control problems, particularly one concerned with near-term problems.

As remarked earlier, the feasibility question should not be prejudiced by the assumption that large amounts of data are absolutely essential for the performance of these functions in a post-attack environment. This issue cannot be settled one way or the other at this moment, but there is strong reason to believe that even small amounts of data, carefully selected and handled fast and reliably by a relatively austere system, could contribute enormously to flexibility of response compared to the performance of a preplanned system with a totally vulnerable command and communications structure. And such relatively small demands for data collection, transmission and processing might be met reliably by various "exotic" means that would not be suitable for peacetime tasks requiring high capacity.

The most important point to be made on the subject of effectiveness is that it demands a research effort on a very much broader front than "command and control" alone. Effectiveness must be judged relative to strategic objectives, and the very feasibility of the objectives most pertinent to command control system design -- objectives such as stability, improved war outcome, rational wartime control of forces -- remains to be established, a task that calls for investigation of

prospects for counterforce tactics, active and passive defenses, threat strategies, and enemy posture and strategy, as well as command and control capability. Until such an overall feasibility analysis can dislodge entrenched beliefs in "deterrence only" and the "spasm war" pattern, it would be hard to generate a real interest in post-attack control.

Even once the feasibility and desirability of more ambitious strategic objectives are accepted, the effectiveness of given command and control structures must be studied in an elaborate context of other factors, with close attention to interactions, trade-offs and mutual constraints among them. These can be divided into:

(1) Factors that the U. S. can control: e.g.,

(a) size, posture and flexibility of offensive forces;

(b) the nature and effectiveness of passive defenses (including fallout protection and the location of strategic bases in relation to cities) and active defenses;

(c) the reliability and survivability of warning and bomb damage reporting systems;

(d) the nature and survivability of command and control hardware (communication means, computers, displays, headquarters facilities);

(e) U. S. strategic doctrine and war plans (their variety, flexibility, concept of the military objectives);

(f) U. S. military posture and procedures (basing, deployment, varieties of alert status, automaticity of response);

(g) information structure (sources of information, variety, reliability, distribution);

(h) counterforce hardware (reconnaissance/surveillance capability, fast-response forces, large warheads and

accurate delivery means; "counterforce capability" in a larger sense will depend on some of the enemy choices listed below).

(2) Factors that the U. S. cannot control: e.g.,

(a) enemy offensive forces;

(b) enemy tactics and "competence";

(c) enemy command and control hardware (e.g., is an enemy commander likely to remain alive, in communication and in control of his forces, despite U. S. retaliation against military targets and/or cities?);

(d) enemy doctrine, military objectives, war plans (is an enemy first strike likely to include many U. S. cities or to hit purely military targets? Does he plan to withhold forces, to implement threat-strategies?

(e) enemy information structure (will an enemy commander have prompt information on the effects of his attack, on remaining U. S. capabilities, on the pattern of U. S. retaliation, on his own remaining capabilities?)

(f) circumstances of the start of the hostilities (e.g., by enemy pre-emptive strike on a false alarm, by escalation from a limited war, by enemy preventive strike in a time of tension, a time of non-tension, by an enemy strike which gives tactical warning or which achieves total surprise, by an accident or unauthorized action on either side, by a U. S. pre-emptive strike on tactical warning or on a false alarm).

All these factors will condition the feasibility and effectiveness of a "war-fighting" capability in general, including, besides post-attack command control, counterforce capability, active and passive defense, and all plans and measures designed to improve the civil and military outcome of a war. Indeed, the interaction between many of these factors is so marked that it is impossible to study the feasibility or usefulness, say, of various command and control systems, in isolation.

This point can be put very strongly, to emphasize the importance of a joint approach to these problems, in the process of analysis and design.

The mutual constraints are such that almost any one of these elements can "fail" to a degree for which the other elements may not be able to compensate: i.e., in a way which may determine an unfavorable outcome. In fact, it is beyond question that under certain possible configurations of the above factors, no post-attack control capability could markedly improve the outcome of the war.

Consider the following hypothetical (and hopefully, unlikely) sets of circumstances:

(1) Enemy forces, tactics and competence, the vulnerability of U. S. forces and the circumstances of war initiation are such that the enemy attack practically wipes out the U. S. offensive force at the outset of war; the command system has nothing significant left with which to fight or threaten.

(2) The U. S. totally lacks any fall-out protection or survivable action defenses, its bases and missile sites are all near cities, and the enemy launches an effective "obliteration" first strike against both U. S. population targets and strategic forces; whether or not the command system survives, the nation it serves is destroyed.

(3) Enemy forces are well hidden or invulnerable to U. S. counter-force tactics, they are governed by a decentralized, all-out commitment doctrine, and the enemy information structure and command control system collapses utterly under the initial U. S. retaliatory strikes; the command system is no longer able to influence enemy action by counterforce or threats.

Even under these circumstances, a survivable command system might prove to have been worth its cost (assuming the cost were modest), but

its contribution to national objectives would clearly be marginal. This is to say that even an "ideal," perfect command and control system -- offering invulnerable, instantaneous, omniscient decision-making and communication -- could not promise to improve the outcome of a war significantly all by itself, so long as situations like the above might arise. Certainly the first situation described above should not be possible if the U. S. makes appropriate decisions; the next two depend more heavily on enemy choices, though these are not beyond our influence. The point is that decisions made in many other sectors, some of them controlled by the enemy and many of them hard to influence or predict, are critical to the scope of contribution which a command system alone can make to national objectives. They could cut that contribution very low, or even deny its feasibility. If that is not to happen, an integrated approach to policy in many areas is needed; and even that might not guarantee the effectiveness of flexible control or of "war-fighting" capability in general.

But such a guarantee should not be required. We are not interested only in the worst cases, or even, exclusively, the most likely cases; we may find a capability worthwhile as "insurance" even for improbably favorable cases. And there are many circumstances other than those above -- and even more plausible, if the U. S. takes appropriate action -- in which a reliable post-attack control capability could prove of inestimable importance. We have considered many of these in earlier sections. The likelihood of such circumstances (even if it were small) could more than justify a major effort to achieve this capability. We have dwelt on the unfavorable cases here only to make clear that feasibility and effectiveness

questions must be recognized as serious and pertinent.

One useful way to approach this problem might be to generate some detailed scenarios of wars beginning under different circumstances, "histories of future wars," detailed enough in sequence and pattern to allow reasonable guesses as to the command alternatives that might be present at given points in the sequence, and the difference that various structures of command, communications and information might make at these points.

We are in no position, prior to such research, fully to anticipate its results. Questions of centralization vs. decentralization, the appropriate hardness of given components, the precise nature and amount of information it would be desirable and/or feasible to supply specified levels of command, cannot be answered here. If this paper has any implication for action, it is primarily to motivate such study. Hopefully, enough has been said to indicate the urgent desirability of some form of survivable, post-attack control capability, at least as a goal of research and system design.

The ability to respond flexibly and adaptively in terms of U. S. national interests, in wartime as in peacetime, bringing to bear upon that response the highest national centers of authority, experience and information both military and political: this might well be regarded as something more than a means. It can be argued that it deserves place among our major national objectives. It is, in any case, prerequisite to other important objectives. This is not to deprecate the relevance of feasibility and cost obstacles, but to urge the importance of efforts to surmount them. It is important to be quite conscious of the

limitations of "collapsible," totally inflexible systems, possibly unreliable and accident-prone, capable at most of a few stereotyped responses, as solutions to "command and control" problems of the next two decades. Whether or not it will prove possible to transcend these special limitations in the next few years, it is urgent to try to do so, to recognize their constraints on national objectives and strategy as highly undesirable even in the short run and unacceptable as present proposals for the long run.

This is to reject the view that it is really "all right" for commanders to die and for the command and communications structure to collapse at the outset of major war. It is to deny that the first thermonuclear war will prove so predictable or simple as that attitude implies; or that one can afford to assume, at the very outset of system design, that given control functions are "impossible." It is to reject the concept of the "spasm war" as the basis of planning for the future.

The actual consequences and effectiveness of a protected command system for post-attack control will remain highly uncertain. There is no way to guarantee that it will prove to have been worth the investment; even a sophisticated, reliable system could not help one make good responses if there were none available. But the consequences of not possessing such a capability seem less uncertain, and intolerably ominous. A command system that could not survive the onset of hostilities, that could not make choices under attack, would offer no hope of meeting the challenges and objectives we have considered; and such hope seems well worth paying for.

REFERENCES

1. Wohlstetter, A. J., "The Delicate Balance of Terror," Foreign Affairs, January, 1959.

2. Kahn, H., "Three Lectures on Thermonuclear War," Princeton University Press, 1960. To be published.

3. Rowen, H. S., National Security and the American Economy in the 1960's, Study Paper No. 18, Joint Economic Committee, Congress of the United States, January 30, 1960.

4. Schelling, T. C., The Strategy of Conflict, Harvard University Press, 1960.

5. Ashby, W. R., Design for a Brain, Wiley, 1960.